Estudio de los puntos de acceso inalámbricos 802.11 en la ciudad de Cali usando las técnicas WAR-X

Andrés F. Millán
Ronald Daza
James Campiño
Universidad Santiago de Cali
Grupo de Investigación COMBA I+D
comba@usc.edu.co

Fecha de recepción: 10-01-2006
Fecha de aceptación: 20-04-2006

ABSTRACT
Hackers can decrypt and read data on a wireless link protected by built-in WEP encryption, and may even able to access the data on a wired network through a Wi-Fi access point. The authors assess Wi-Fi network security in on Santiago de Cali (Colombia) city used War-X techniques

KEY WORDS
Santiago de Cali, WarDriving, WarWalking, War-X, Wi-Fi Networks., Wireless Networks Security.

RESUMEN
Los hackers pueden desencriptar y leer datos en conexiones inalámbricas protegidas por encriptación WEP (encriptación inalámbrica del estándar básico 802.11), además pueden tener la capacidad de acceder a datos de la red cableada a través de un punto de acceso Wi-Fi. Los autores estudiaron la seguridad de las redes Wi-Fi en la ciudad de Santiago de Cali (Colombia) usando las técnicas War-X.

PALABRAS CLAVE
Redes Wi-Fi, Santiago de Cali, seguridad en redes inalámbricas, WarDriving, Warwalking, War-X

Clasificación Colciencias: A

1. INTRODUCCIÓN

Las redes inalámbricas Wi-Fi (basadas en los estándares 802.11), han aumentado su popularidad en los últimos años. Muchos usuarios están instalando redes Wi-Fi en sus casas para acceder a sus servicios de red de banda ancha o imprimir sus documentos desde cualquier lugar de su hogar. Igualmente numerosas empresas han adicionado puntos de acceso Wi-Fi a sus redes cableadas, extendiendo la conectividad de sus empleados en sus servicios de redes corporativos. Sin embargo, la proliferación de las redes Wi-Fi también ha dado a los hackers nuevas oportunidades para obtener acceso no autorizado a los sistemas empresariales o a los datos confidenciales de usuarios residenciales y empresas.

Lo más preocupante es que la mayoría de las debilidades de las implementaciones Wi-Fi no se originan en la escasez de arquitecturas o tecnologías de seguridad para los ambientes inalámbricos, sino en la falta de conocimiento de los usuarios y las empresas de los nuevos requerimientos y amenazas a la seguridad que nacen de la instalación de redes Wi-Fi.

El grupo de investigación COMBA I+D, consciente de la necesidad de promover entre los usuarios colombianos una cultura hacia la seguridad inalámbrica, realizó un estudio de los puntos de acceso inalámbricos Wi-Fi en la ciudad de Cali utilizando las técnicas de War-X, con el propósito de conocer el estado actual, cantidad, localización y seguridad de los puntos de acceso inalámbricos existentes.

Este artículo está dividido en tres partes, primero se introduce a las técnicas de War-X, luego se detalla el procedimiento y herramientas utilizados para realizar el estudio, luego se analizan los datos usando una plataforma Web desarrollada por el grupo investigador. Por último se presentan unas recomendaciones y conclusiones que se pueden utilizar para aumentar los niveles de seguridad de las redes Wi-Fi en las empresas y los hogares.

2. LAS TÉCNICAS DE DETECCIÓN INALÁMBRICA WAR-X

Los hackers inalámbricos especializados en redes Wi-Fi emplean varias técnicas para detectar hotspots inalámbricos o zonas de cobertura de red local inalámbrica. Uno de los grupos de técnicas más utilizados para realizar ataques recibe el nombre de War-X. War-X hace relación a un conjunto de técnicas pasivas de detección de redes Wi-Fi. La Tabla 1 resume las derivaciones de las técnicas War-X.

Las técnicas War-X explotan la emisión repetitiva de mensajes de broadcast enviados por los puntos de acceso inalámbricos. Estos mensajes broadcast son usados por los puntos de acceso inalámbricos para localizar y permitir la conexión a la red de todos los usuarios de una manera simple. Sin embargo estos mensajes broadcast contienen información sensible para la seguridad de la red Wi-Fi como son el identificador de la red Wi-Fi (denominado SSID), la dirección MAC y la configuración de la encriptación del punto de acceso inalámbrico, entre otros.

Aunque estas técnicas son utilizadas por hackers para buscar redes Wi-Fi vulnerables, el objetivo de este estu-

Tabla 1. Técnicas War - X

Nombre de las técnicas	Descripción
WarDriving	Detección utilizando un vehículo para mapear las casas y empresas que tienen redes Wi-Fi, utilizando software instalado en un portátil inalámbrico.
WarWalking	Detección que envuelve caminar por un vecindario o un centro comercial, utilizando un PDA con conexión inalámbrica.
WarSkating	Detección utilizando patines
WarCycling	Detección utilizando bicicletas
WarFlying	Detección utilizando aviones o helicópteros

dio no era aprovecharse de dichas vulnerabilidades mediante ataques activos, sino simplemente conocer específicamente el estado actual de la seguridad de dichos nodos de red Wi-Fi.

El grupo investigador decidió utilizar la técnica de WarDriving para cubrir de manera rápida el área de detección seleccionada y el uso WarWalking para visitas de detección específicas sobre todo en grandes superficies como supermercados, centros comerciales, etc.

3. USANDO WAR-X EN LA CIUDAD DE CALI

El primer paso antes de aplicar las técnicas War-X es seleccionar el área de detección, el grupo investigador seleccionó las comunas 2, 3, 4, 8, 9, 10, 17 y 19 de la ciudad de Cali, tomando como criterio de selección aquellas con la mayor cantidad de instalaciones de servicios de banda ancha y de redes de acceso corporativas de un operador de telecomunicaciones local.

Posteriormente se realizó un estudio explorativo de las actividades de War-X en el ámbito internacional encontrando proyectos referentes como la iniciativa WWWD (World Wide War Drive) en los Estados Unidos, o estudios específicos realizados en Chile, Argentina, España y Japón, entre otros. En Colombia se conoce de dos estudios con poco alcance en las ciudades de Medellín y Bogotá.

De acuerdo con las experiencias de WarDriving en otros países, el grupo investigador se equipó con un portable con una tarjeta inalámbrica 802.11b conectada a una antena externa de gran ganancia, junto a un sistema GPS de uso civil. La Figura 3 muestra el equipamiento seleccionado para realizar el estudio de WarDriving. Para el estudio de áreas específicas con WarWalking se utilizó una PDA con conectividad inalámbrica Wi-Fi.

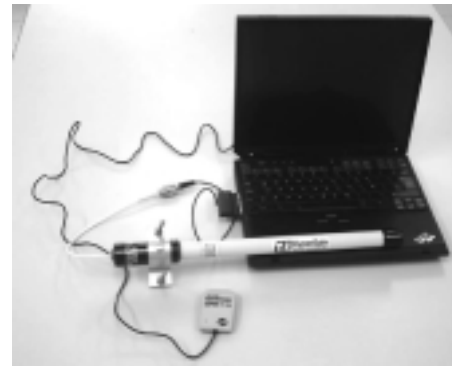

Figura 1. Equipos utilizados para el estudio de WarDriving.

Además del hardware requerido es necesario un software de detección,

según sistema operativo instalado en el portable, hoy día en Internet es posible tener una amplia colección de herramientas de software para detectar redes Wi-Fi, capturar paquetes o «crakear» las claves WEP. Por ejemplo, para el sistema operativo MacOS encontramos herramientas como KisMAC (http://kismac.com) o MacStumbler (www.macstumbler.com). En los sistemas operativos Linux y BSD hallamos Kismet (www.kismetwireless.net) y AirSnort (http:// airsnort.shmoo.com). El grupo investigador decide utilizar tres herramientas con soporte para sistema operativo Windows XP de Microsoft, como software de descubrimiento de redes Wi-Fi NetStumbler (para el portable) y MiniStumbler (para la PDA), además de un software GIS para la ubicación de los puntos de acceso sobre un mapa cartográfico denominado DivaGIS. La Figura 2 muestra el esquema de conexión seleccionado para realizar el estudio de WarDriving.

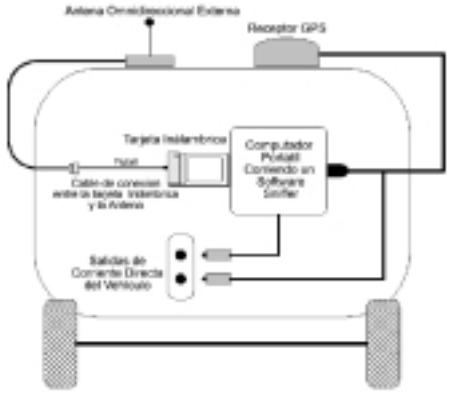

Figura 2. Esquema de conexión del hardware y software en el vehículo.

Por último, el grupo investigador realizó salidas programadas en el área de detección seleccionada. Es importante aclarar que el WarDriving no es una técnica ilegal mientras no se establezca una conexión a las redes detectadas sin permiso del dueño. Sin embargo en algunas ocasiones los adaptadores usados se pueden «autoconectar» a los puntos de acceso inalámbrico, por eso es recomendable desactivar los protocolos de red del adptador inalámbrico como TCP/IP.

4. RESULTADOS DEL ESTUDIO

El proyecto tenía como uno de sus objetivos específicos el diseño y construcción de una herramienta Web que sirviera como motor estadístico de los resultados obtenidos en este estudio, así como en futuros trabajos, además de permitir divulgar los resultados en Internet. La Figura 3 muestra una pantalla del software denominado WDCali, en esta herramienta se pueden almacenar las estadísticas por cada salida, por cada estudio y realiza gráficas estadísticas de los principales aspectos de la seguridad y configuración de los puntos de acceso inalámbricos Wi-Fi

Cuando el grupo investigador inició el presente estudio, estimó que la cantidad de puntos de accesos inalámbricos 802.11 existentes en Cali no sobrepasaría las 100 unidades, sin embargo durante la detección usando War-X se encontraron 522 puntos de acceso inalámbricos. La Figura 4 muestra los puntos detectados por cada una de las comunas caleñas seleccionadas.

Al analizar los resultados se puede llegar a varias conclusiones:

- La cantidad de puntos de acceso que tienen configurado WEP es de 319 unidades, lo cual representa el 61.1% del total; sin embargo, al-

Figura 3. Herramienta Web denominada WDCali para la presentación de los resultados del estudio.

Figura 4. Distribución de los puntos de acceso inalámbricos Wi-Fi detectados en Cali.

gunos de los puntos inalámbricos configurados WEP están por defecto, además el protocolo WEP no es confiable si no se utilizan políticas de actualización de la clave (WEP dinámico).

- La cantidad de puntos de acceso que envían el SSID es muy alta, con el 96% del total detectado, es decir, 476 unidades. Esta cifra demuestra lo poco sensibilizados que están los usuarios de los riesgos de las redes Wi-Fi.
- La cantidad de puntos de acceso configurados por defecto es importante con cerca del 20.6%, estas 102 unidades señalan una tendencia mundial de instalar las soluciones Wi-Fi que propenden a ser tecnologías «plug and play» sin realizar ninguna configuración adicional, en palabras sencillas: «Que funcione es lo importante».
- Las comunas con más puntos de acceso inalámbricos detectados son la 2 y la 17, áreas de la ciudad habitadas por una población de clase media-alta y alta. Ade-

más, la comuna 2 es el área con mayor oferta de redes de banda ancha para los usuarios residenciales (DSL, HFC) lo cual favorece el uso de puntos de acceso inalámbrico Wi-Fi para compartir los recursos de Internet en el área de cobertura de un hogar o de varios residentes.

- El canal más usado para configurar los puntos de acceso inalámbricos es el 6, lo cual representa el 41,9% del total.
- La cantidad de puntos de acceso inalámbrico con tecnología 802.11g es sobresaliente con un 44%, es decir, 217 unidades. Esto muestra una buena oferta de productos Wi-Fi de última generación por parte de los distribuidores.

Basándonos en el SSID, se puede decir que la mayoría de los puntos de acceso inalámbrico están instalados en residencias o edificios de apartamentos, lo cual muestra que uno de los sectores de mayor interés en la ciudad para la oferta de servicios de telecomunicaciones de banda ancha es el residencial. El sector empresarial también demuestra interés por las soluciones inalámbricas Wi-Fi en especial para ofrecer conectividad LAN a sucursales u oficinas pequeñas, para áreas de salas de reuniones y para realizar conexiones punto a punto en ambientes metropolitanos.

La Tabla 2 resume los resultados alcanzados en el estudio.

Tabla 2. Resumen del estudio utilizando War-X.

Item	Total	(%)
Redes ad-hoc	22	4.2
Redes BSS (AP)	496	96
AP'S que envian SSID	476	96
AP'S sin encriptación	203	40.9
AP'S S config. X defecto	102	20.6
Canal más usado	6	41.9
Total de detecciones	522	
AP'S 802.11B	276	56
AP'S 802.11G	217	44

5. OPCIONES DE SEGURIDAD INALÁMBRICA

5.1. Wi-Fi Protected Access (WPA)

WPA es un estándar desarrollado por la alianza Wi-Fi, el cual incluye mejores especificaciones para la autenticación, control de acceso, integridad y privacidad del mensaje y distribución de llaves en los sistemas Wi-Fi existentes. El estándar está diseñado para funcionar como una actualización del software y es compatible con el estándar 802.11i del grupo de trabajo 802.11.

Para proveer protección al mensaje, WPA utiliza TKIP (Temporal Key Integrity Protocol) cuyo objetivo es resolver las deficiencias de WEP ofreciendo una defensa contra el reúso de claves, la modificación del mensaje y los ataques basados en la repetición de mensajes para buscar la clave. WPA también implementa una autenticación basada en EAP (Extensible Authentication Protocol) y en el control de acceso basado en la arquitectura 802.1x, la cual hace uso de un servidor de autenticación RADIUS (Remote Authentication Dial-in User) para autenticar cada usuario en la red.

Es recomendable para las empresas emplear WPA con autenticación basada en 802.1x y EAP utilizando un servidor RADIUS. Para los hogares y empresas pequeñas que no cuentan

en su mayoría con servidores RADIUS, se debe usar el modo de *pre-shared key* (clave previamente compartida), con la cual el usuario debe ingresar un password desde la estación móvil para poder conectarse a la red. Esto subraya la necesidad de cuidar las claves WEP: seleccionando claves complejas de «crakear» (se debe escoger preferiblemente claves que incluyan caracteres de los cuatro conjuntos de caracteres) y evitando el mal uso de las claves (por ejemplo cuando se dan a conocer las claves a terceros).

5.2. Redes Privadas Virtuales (VPNs)

Las redes privadas virtuales son túneles de conexión privadas sobre la infraestructura de red inalámbrica, estos sistemas de entunelamiento usan varias técnicas de encriptación que aseguran la confidencialidad de la información como 3DES o AES. Las redes VPN requieren que el usuario tenga instalado en su terminal móvil un cliente VPN que se comunica con un software de servidor VPN que corre en el equipo que ofrece los servicios de red.

Debido a su complejidad, el uso de redes privadas virtuales es recomendado para empresas, sin embargo los administradores y jefes de seguridad informática de las compañías deben estar conscientes de los problemas de incompatibilidad (múltiples sistemas como L2TP, IPSec, PPTP, MSCHAP, entre otros) y limitaciones de las implementaciones de VPN, por ejemplo que si un usuario desea conectarse con varios servidores se debe establecer un túnel por cada servidor, lo cual es ineficiente y consumista del ancho de banda disponible.

5.3. Portales captativos

Un portal captativo es un enrutador o una pasarela, que no permite el paso de tráfico de red antes de la autenticación del usuario. El portal captativo funciona en varias pasos: 1) Un servidor DHCP envía una dirección IP al cliente móvil usando la conexión Wi-Fi, 2) El tráfico es bloqueado, excepto el servidor del portal captativo en la red cableada, 3) Redirecciona todo el tráfico Web del cliente móvil hacia el portal captativo, 4) Retorna la página Web que despliega los términos de uso, información del pago o la pantalla de login y 5) Cuando el usuario acepta los términos o ingresa su password, entonces se le permite el acceso.

Los portales captativos son una solución ideal para los operadores de telecomunicaciones inalámbricos que desean ofrecer cobertura inalámbrica Wi-Fi usando hotspots, pues con estos portales se establece un sistema de seguridad aceptable y fácil de usar, además que es posible implementar sistemas de valor agregado como portales inteligentes basados en localización, por ejemplo en un centro comercial un portal captativo podría ofrecer promociones de los productos y servicios de los almacenes del centro comercial. Sin embargo, el intercambio de passwords y páginas seguras requiere el uso de protocolos como SSL y SSH o de firewall personales que hacen más compleja la configuración para los clientes de la red inalámbrica.

6. CONCLUSIONES Y PROYECTOS FUTUROS

La ciudad de Cali no ha sido ajena al interés mundial por las tecnologías

inalámbricas Wi-Fi, que sin duda al juzgar por los hallazgos de este estudio estarán pronto en muchos hogares de los colombianos y específicamente de los caleños. Dicha tendencia nos enfrenta a un nuevo reto de promover el desarrollo de una cultura de seguridad informática para estos nuevos entornos inalámbricos.

Los usuarios de redes Wi-Fi tienen nuevas alternativas de seguridad para sus infraestructuras como: WPA (Wireless Protected Access) con compatibilidad a 802.11i, las redes privadas virtuales (VPN) inalámbricas y los portales captativos. Sin embargo, lastimosamente no hay una solución inalámbrica universal a los problemas de seguridad y aunque WPA y las redes VPN tienen mucho potencial, a menudo crean problemas de configuración e interoperabilidad a los usuarios.

Conscientes de esta situación y del estado actual de los puntos de acceso inalámbrico de la ciudad de Cali, el grupo de investigación COMBA I+D ha decidido iniciar dos proyectos, primero el desarrollo de un curso-taller corto dirigido a usuarios no técnicos sobre aspectos de seguridad de las redes 802.11 y el segundo, un proyecto que lleve a una arquitectura de seguridad adecuada a los entornos residenciales y pymes utilizando herramientas GNU o propias.

BIBLIOGRAFÍA

1. Vladimirov, Andrew, Gavrilenko, Konstantin, Mikhailovsky, Andrei. «WI-FOO. The Secrets of Wireless Hacking». Addison-Wesley. Pearson Education. Agosto 2004.
2. Daza, Ronald, Campiño, James. «WarDriving: ¿El preludio de un ataque inalámbrico?». Proyectos de curso COMBA I+D. Universidad Santiago de Cali. Noviembre 2004.
3. Hole, Kjell, Dyrnes, Erlend, Thorsheim, Per. «Securing Wi-Fi Networks». *IEEE Computer Magazine.* IEEE. Julio 2005.
4. Gast M. S. «802.11 Wireless Networks: The Definitive Guide». O'Really. 2002
5. Edney J, Arbaugh W.A. «Real 802.11 Security:Wi-Fi Protected Access and 802.11i». Addison Wesley.2004.
6. Potter B., Fleck B., «802.11 Security». O'Really. 2003.

CURRÍCULOS

Andrés Felipe Millán Cifuentes
Ingeniero de Sistemas de la Universidad Icesi de Cali. Máster en Sistemas y Redes de Comunicaciones, Universidad Politécnica de Madrid, España. Profesor Titular de la Universidad Santiago de Cali. Director del grupo de investigación COMBA I+D. Miembro de IEEE Communications. Miembro del consorcio I2COMM. Sus áreas de investigación son las redes inalámbricas, las redes de banda ancha y la computación móvil.

James Campiño y Ronald Daza
Ingenieros de Sistemas y Telemática de la Universidad Santiago de Cali. Proyectistas del grupo de investigación COMBA I+D 2004-2006